
Universidad Católica
"Nuestra Señora de la Asunción"

Facultad de Ciencia y Tecnología

Teoría y Aplicación de la
Informática 2

# Tecnologías VPN

María Soledad Marecos Ortiz

2010

# Introducción

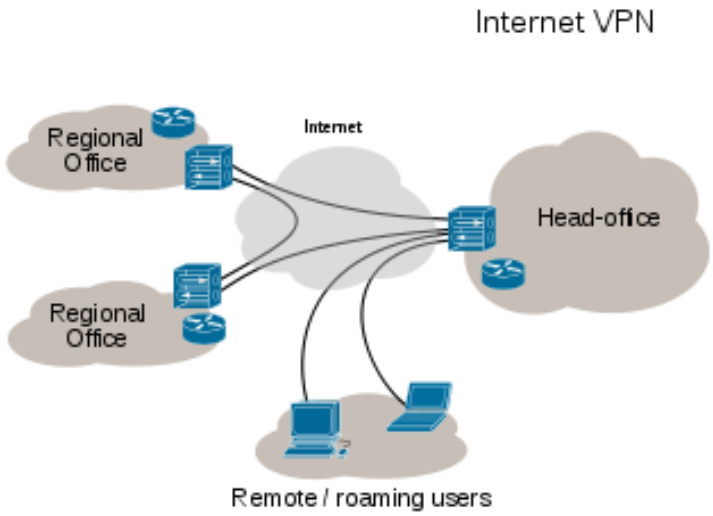
La aparición de Internet revolucionó la vida, los métodos y estrategias antes conocidas por el ser humano para comunicarse, relacionarse, hacer negocios, etc, e incluso en la actualidad sigue generando controversias de todo tipo.

A comienzos del siglo XXI, cuando internet aun seguía sufriendo grandes transformaciones, las empresas que buscaban servicios de red de los proveedores para apoyar su intranet y los proveedores de servicios que buscaban satisfacer esta demanda de los clientes mediante la construcción de redes globales cada vez más integradas con la intencion de ofrecer a los clientes soluciones completas de servicios adaptados a sus negocios particulares, dieron lugar a lo que hoy conocemos como VPN (Red Privada Virtual).

El incremento de la demanda de aplicaciones ricas en funcionalidades y una fuerza de trabajo ampliamente dispersa, obligaron a empresas de todos los tamaños, a replantear sus estrategias de red. Los desarrolladores de redes siguieron buscando formas de conectar sitios dispersos a intranets corporativas cada vez de mayor tamaño, de manera eficiente y rentable. Las empresas necesitaban expandir su alcance para incluir a socios y proveedores, y a medida que el número de usuarios remotos crece, la creación de una empresa distribuida se vuelve aún más difícil, razón por la cual éstas redes privadas virtuales son un excelente ejemplo de los servicios mundiales que benefician tanto a nuevos clientes empresariales como a los proveedores de servicios.

# VPN - Virtual Private Network (Red Privada Virtual)

## VPN




Una red privada virtual - VPN (Virtual Private Network), es una tecnología de red que permite a sus usuarios, extender su red local sobre una red pública. Es un ejemplo de red WAN (red de área amplia).

Utiliza una infraestructura pública de telecomunicaciones y tecnologías como el Internet, para proporcionar a las oficinas remotas o usuarios individuales, acceso seguro a la red de su organización. Su intención es evitar un costoso sistema de arrendamiento o compra de líneas, que será utilizada por una sola organización.

El objetivo de una VPN es ofrecer a la organización las mismas capacidades de seguridad, pero a un menor costo. Encapsula las transferencias de datos entre dos o más dispositivos en red, que no se encuentran en la misma red privada, a fin de mantener los datos transferidos, privados de otros dispositivos. Hay muchas clasificaciones diferentes, implementaciones y usos para VPNs.

Algunos ejemplos son: la posibilidad de interconectar dos o más sucursales de las empresa utilizando Internet como medio, permitir a los usuarios del departamento de asistencia técnica la conexión desde sus casas al centro de cómputo, que los usuarios pueda tener acceso a su equipo del hogar desde algún lugar remoto, por ejemplo desde un hotel. Todo esto utilizando sólo la infraestructura de Internet.

## ORÍGEN Y COMIENZOS DE LAS VPN

Hasta finales de la década de 1990 las computadoras se conectaban a la red a través de muy caras líneas arrendadas o líneas de discado telefónico. Podía costar miles de dólares para las líneas de

56kbps o decenas de miles de dólares para líneas T1, dependiendo de la distancia entre los lugares.

Las redes privadas virtuales redujeron los costos de red, ya que evitan la necesidad de muchas líneas arrendadas que se conectan a Internet individualmente. Los usuarios pueden intercambiar datos privados de forma segura, haciendo que las líneas arrendadas sean innecesarias.

Las tecnologías VPN dispusieron de diferentes elementos que las definen, ya sean los múltiples protocolos, las terminologías, influencias de comercialización, etc. Por ejemplo, las tecnologías de VPN pueden diferir en:

- Los protocolos que utilizan para el tráfico del túnel.
- El túnel de punto de terminación, es decir, el borde de los clientes o el borde proveedor de red.
- Ya sea que ofrecen conectividad de acceso de sitio a sitio o remota.
- Los niveles de seguridad que ofrece.

## ARQUITECTURAS VPN

Acceso remoto

Uno de los modelos más usado en la actualidad que consiste en usuarios o proveedores conectados a la central desde sitios remotos (oficinas, comercios, casas, hoteles, aviones, entre otros) utilizando la infraestructura de Internet para acceder a su red. Desde el momento en que son identificados y autenticados poseen acceso parecido al que tienen dentro de la red de la empresa.

Punto a punto

Se utiliza para conectar ordenadores remotos con el servidor central. El servidor VPN, conectado permanentemente a Internet, acepta, a través de esta conexión, aquellas solicitudes provenientes de los sitios identificados y establece el túnel VPN.

*Tunneling*

Técnica que consiste en encapsular un protocolo de red en otro permitiendo tener un túnel la red. El túnel se puede utilizar incluyendo una PDU establecida dentro de otra, con el fin de transmitirla de un extremo a otro sin que sea necesaria la interpretación intermedia de la PDU que fue encapsulada. Así se rutean los paquetes sobre nodos intermedios incapaces de ver el

contenido de estos paquetes. El túnel se define por los extremos y el protocolo de comunicación elegido, que podría ser SSH, o algún otro.

Esta técnica tiene varios objetivos, que dependen del problema abordado, por ejemplo la comunicación en escenarios multicast, redirección de tráfico y otros.

Un ejemplo de uso de esta técnica es en la redirección de tráfico en IP Móvil.

Over LAN

Ésta es la menos difundida de las arquitecturas, pero una de las más poderosas para utilizar dentro de la red local. Es similar a la arquitectura de acceso remoto, pero en lugar de usar Internet como medio para la conexión, usa la misma red de área local. Sirve para aislar zonas o servicios de la red local. Esto lo hace muy útil para mejorar la seguridad de las redes inalámbricas.

Un ejemplo es la conexión a redes WIFI usando en los túneles los cifrados IPSEC, SSL, u otro, que además de utilizar los métodos de autenticación normales, agregan credenciales de seguridad del túnel VPN en la red local.

## ESTRUCTURAS Y REQUERIMIENTOS DE LAS VPN

Las maneras de comunicación existentes para conectar las partes de la red privada sobre las redes públicas, se realiza estableciendo el tunneling entre dos puntos para los que se negocian sistemas de encriptación y autenticación que garantizan la confidencialidad e integridad de los datos privados que se transmiten sobre la red pública. Debido a que se utilizan redes públicas, por lo general Internet, se necesita prestar mayor atención a cuestiones de seguridad, que son tenidos en cuenta a través de los esquemas de encriptación y autenticación.

Los métodos de autenticación son inprescindibles en las VPNs, ya que dan a los participantes de la misma la seguridad de estar intercambiando información con los dispositivos o usuarios deseados. La autenticación en las VPNs se realiza de manera similiar al inicio de sesión en algún sistema con nombre de usuario y contraseña, pero con mayores restricciones de validación de identidad. La mayor parte de los sistemas de autenticación utilizados en VPN están basados en claves compartidas.

La autenticación se lleva a cabo por lo general, al comienzo de la sesión, y posteriormente de manera aleatoria durante el transcurso de ésta, para asegurar de que no exista ningún participante entrometido en la conversación. Además, la autenticación puede tambien ser utilizada para confirmar la integridad de los datos enviados y recibidos. Los datos se procesan con la ayuda de algún algoritmo de hash para obtener el valor del mensaje como checksum. Cualquier alteración en el checksum nos indica que los datos fueron corruptos o modificados en la transmisión o por el camino.

Algunos ejemplos de algoritmos de autenticación son el Challenge Handshake Authentication Protocol (CHAP) y el algoritmo de alta popularidad en redes, RSA.

Todas las VPNs poseen algún mecanismo de encriptación, que en principio, lo que hacen es empaquetar los datos en un paquete confiable y seguro. La encriptación se considera tan importante como la autenticación, ya que permite que los datos transportados no sean visualizados o interpretados en el trayecto de extremo a extremo. Los métodos existentes para encriptar utilizados en VPNs, son los comunes en redes: encriptación de clave privada y de clave pública.

La encriptación de clave secreta usa una clave dada a conocer solo a los usuarios autorizados a acceder a la información encriptada. Esta clave es utilizada para encriptar como para desencriptar los datos. Esta encriptación tiene el problema de que la clave debe ser compartida por todos los usuarios y al mismo tiempo debe mantenerse en secreto, si fuera revelada, debe ser cambiada y distribuida nuevamente entre los usuarios, por lo que puede filtrarse la clave, y de esta forma ocasionarnos dificultades en la seguridad, razón por la cual, se recomienda la encriptación de clave pública que implica el uso de dos claves, una pública y una privada. La pública es enviada a todos los participantes. Para encriptar, se utiliza la clave privada del emisor y la clave pública del otro participante para encriptar. Al recibir los datos, éstos son desencriptados utilizando la clave privada del receptor y la clave pública del emisor. La única desventaja de esta encriptación es que puede ser menos rápida que la de encriptación de clave secreta, teniendo en cuenta que la encriptación en las VPNs debe ser en tiempo real.

Uno de los protocolos más utilizados para encriptar en VPNs es IPSec, que es en un conjunto de propuestas del IETF que enmarcan un protocoloIP seguro para IPv4 e IPv6. IPSec provee encriptación y por lo tanto seguridad a nivel de paquetes IP.

El tunneling, como fue descrito anteriormente, es una de las formas de crear una VPN. Permite a la red encapsular paquetes dentro de otros paquetes para relacionar protocolos que no son compatibles. Entre los protocolos que utilizados para esta metodología están los protocolos PPTP (Point-to-Point Tunneling Protocol), L2FP (Layer-2 Fowarding Protocol) y también el modo tunel que posee IPSec.

## PROTOCOLOS UTILIZADOS EN LAS VPN

PPTP

Point-to-Point Tunneling Protocol fue desarrollado por Ascend Communications, 3Com Corporation, U.S. Robotics, Microsoft, y ECI Telematics para brindar acceso remoto y a servidores de red a los clientes de una red privada virtual.

PPTP, como uno de los protocolos de túnel, encapsula los paquetes de cualquiera de los protocolos de red en paquetes IP, los cuales posteriormente son tratados como cualquier otro paquete IP. La gran ventaja de este tipo de encapsulamiento es que cualquier protocolo puede ser ruteado a través de una red IP, como por ejemplo Internet.

El diseño de PPTP se debió a la necesidad de permitir que los clientes se conecten a un servidor RAS sin importar su ubicación, a través de su conexión a Internet para poder los accesos como hicieran las solicitudes directamente al servidor al que accede comunmente. En vez de discar a un modem conectado al servidor RAS, los usuarios se conectan a su proveedor y luego "llaman" al servidor RAS a través de Internet utilizando PPTP.

Describimos dos escenarios para estas VPN:

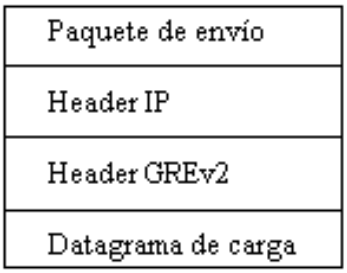
- Un usuario remoto se conecta a un ISP que provee el servicio de PPTP hacia el servidor RAS.
- El usuario remoto se conecta a un ISP que no provee el servicio de PPTP hacia el servidor RAS y, por lo tanto, debe iniciar la conexión PPTP desde su propia máquina cliente.

Para el primero de los escenarios, el usuario remoto estable una conexión PPP con el ISP, que luego establece la conexión PPTP con el servidor RAS. Para el segundo escenario, el usuario remoto se

conecta al ISP mediante PPP y luego "llama" al servidor RAS mediante PPTP. Luego de establecida la conexión PPTP, para cualquiera de los dos casos, el usuario remoto tendrá acceso a la red corporativa como si estuviera conectado directamente a la misma.

La técnica de encapsulamiento de PPTP se basa en el protocolo Generic Routing Encapsulation (GRE), que puede ser usado para realizar túneles para protocolos a través de Internet. La versión PPTP, denominada GREv2, añade extensiones para temas específicos como Call Id y velocidad de conexión.

El paquete PPTP está compuesto por un header de envío, un header Ip, un header GREv2 y el paquete de carga. El header de envío es el protocolo enmarcador para cualquiera de los medios a través de los cuales el paquete viaja, ya sea Ethernet, frame relay, PPP. El header IP contiene información relativa al paquete IP, como ser, direcciones de origen y destino, longitud del datagrama enviado, etc. El header GREv2 contiene información sobre el tipo de paquete encapsulado y datos específicos de PPTP concernientes a la conexión entre el cliente y servidor. Por último, el paquete de carga es el paquete encapsulado, que, en el caso de PPP, el datagrama es el original de la sesión PPP que viaja del cliente al servidor y que puede ser un paquete IP, IPX, NetBEUI, entre otros. La siguiente figura ilustra las capas del encapsulamiento PPTP.




Para la autenticación, PPTP tiene tres opciones de uso: CHAP, MS-CHAP y aceptar cualquier tipo, inclusive texto plano. Si se utiliza CHAP, standard en el que se intercambia un "secreto" y se comprueba ambos extremos de la conexión coincidan en el mismo, se utiliza la contraseña de Windows NT, en el caso de usar este sistema operativo, como secreto. MS-CHAP es un standard propietario de Microsoft y resulta ser una ampliación de CHAP. Para la tercer opción, el servidor RAS aceptará CHAP, MS-CHAP o PAP (Password Autenthication Protocol), que no encripta las contraseñas.

Para la encriptación, PPTP utiliza el sistema RC4 de RSA, con una clave de sesión de 40 bits.

IPSec

IPSec trata de remediar algunas falencias de IP, tales como protección de los datos transferidos y garantía de que el emisor del

paquete sea el que dice el paquete IP. Si bien estos servicios son distintos, IPSec da soporte a ambos de una manera uniforme.

IPSec provee confidencialidad, integridad, autenticidad y protección a repeticiones mediante dos protocolos, que son Authentication Protocol (AH) y Encapsulated Security Payload (ESP).

Por confidencialidad se entiende que los datos transferidos sean sólo entendidos por los participantes de la sesión.

Por integridad se entiende que los datos no sean modificados en el trayecto de la comunicación.

Por autenticidad se entiende por la validación de remitente de los datos.

Por protección a repeticiones se entiende que una sesión no pueda ser grabada y repetida salvo que se tenga autorización para hacerlo.

AH provee autenticación, integridad y protección a repeticiones pero no así confidencialidad. La diferencia más importante con ESP es que AH protege partes del header IP, como las direcciones de origen y destino.

ESP provee autenticación, integridad, protección a repeticiones y confidencialidad de los datos, protegiendo el paquete entero que sigue al header.

AH sigue al header IP y contiene diseminaciones criptográficas tanto en los datos como en la información de identificación. Las diseminaciones pueden también cubrir las partes invariantes del header IP.

El header de ESP permite rescribir la carga en una forma encriptada. Como no considera los campos del header IP, no garantiza nada sobre el mismo, sólo la carga.

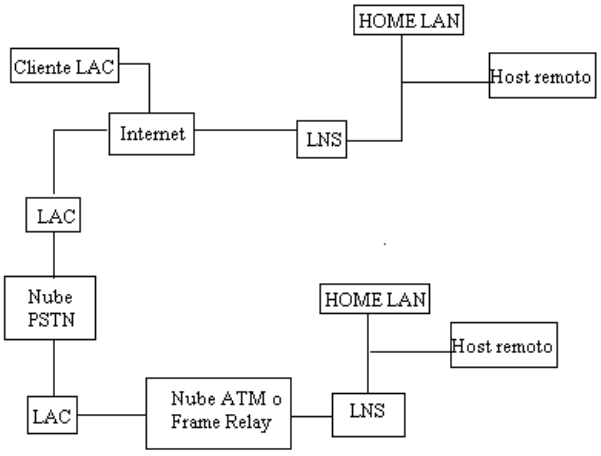
Una división de la funcionalidad de IPSec es aplicada dependiendo de dónde se realiza la encapsulación de los datos, si es la fuente original o un gateway:

- El modo de transporte es utilizado por el host que genera los paquetes. En este modo, los headers de seguridad son antepuestos a los de la capa de transporte, antes de que el header IP sea incorporado al paquete. En otras palabras, AH cubre el header TCP y algunos campos IP, mientras que ESP cubre la encriptación del header TCP y los datos, pero no incluye ningún campo del header IP.
- El modo de túnel es usado cuando el header IP entre extremos está ya incluido en el paquete, y uno de los extremos de la conexión

segura es un gateway. En este modo, tanto AH como ESP cubren el paquete entero, incluyendo el header IP entre los extremos, agregando al paquete un header IP que cubre solamente el salto al otro extremo de la conexión segura, que, por supuesto, puede estar a varios saltos del gateway.

Los enlaces seguros de IPSec son definidos en función de Security Associations (SA). Cada SA está definido para un flujo unidireccional de datos y generalmente de un punto único a otro, cubriendo tráfico distinguible por un selector único. Todo el tráfico que fluye a través de un SA es tratado de la misma manera. Partes del tráfico puede estar sujeto a varios SA, cada uno de los cuales aplica cierta transformación. Grupos de SA son denominados SA Bundles. Paquetes entrantes pueden ser asignados a un SA específico por los tres campos definitorios: la dirección IP de destino, el índice del parámetro de seguridad y el protocolo de seguridad. El SPI puede ser considerado una cookie que es repartido por el receptor del SA cuando los parámetros de la conexión son negociados. El protocolo de seguridad debe ser AH o ESP. Como la dirección IP de destino es parte de la tripleta antes mencionada, se garantiza que este valor sea único. Como en Transport Adjacency, esto autenticaría el paquete completo salvo algunos pocos campos del header IP y también encriptaría la carga. Cuando un header AH y ESP son directamente aplicados como en esta manera, el orden de los header debe ser el indicado. Es posible, en el modo de túnel, hacer una encapsulación arbitrariamente recursiva para que el orden no sea el especificado.

L2TP




Layer-2 Tunneling Protocol (L2TP) da facilidades para el proceso de entunelamiento de datos en paquetes PPP a través de la red de manera tal que sea lo más transparente para los usuarios de los extremos del túnel y sus aplicaciones.

El escenario típico L2TP, cuyo objetivo es la creación de entunelar marcos PPP entre el sistema remoto o cliente LAC y un LNS ubicado en una LAN local, es el que se muestra en la siguiente figura.

Un L2TP Access Concentrator (LAC) es un nodo que actúa como un extremo de un túnel L2TP y es el par de un LNS. Un LAC se sitúa entre un LNS y un sistema remoto y manda paquetes entre ambos. Los paquetes entre el LAC y el LNS son enviados a través del túnel L2TP y los paquetes entre el LAC y el sistema remoto es local o es una conexión PPP.

Un L2TP Network Server (LNS) actúa como el otro extremo de la conexión L2TP y es el otro par del LAC. El LNS es la terminación lógica de una sesión PPP que está siendo puesta en un túnel desde el sistema remoto por el LAC.

Un cliente LAC, una máquina que corre nativamente L2TP, puede participar también en el túnel, sin usar un LAC separado. En este caso, estará conectado directamente a Internet.

El direccionamiento, la autenticación, la autorización y el servicio de cuentas son proveídos por el Home LAN's Management Domain.

L2TP usa dos clases de mensajes: los mensajes de control y los mensajes de datos. Estos mensajes de control son utilizados para establecer, mantener y borrar túneles y llamadas. Usan el canal de control dentro de L2TP para asegurar el envío. Y los mensajes de datos encapsulan los marcos PPP que luego serán enviados por túnel.

Los marcos PPP enviados por del canal de datos no confiable, encapsulado primero por un encabezado L2TP y luego por un transporte de paquetes como UDP, Frame Relay o ATM. Los mensajes de control son enviados a través de un canal de control L2TP confiable que transmite los paquetes sobre el mismo transporte de paquete.

Se requiere que haya números de secuencia en los paquetes de control, que son usados para proveer el envío confiable en el canal de control. Aquellos mensajes de datos pueden utilizar sus números de secuencia para poder reordenar y detectar paquetes perdidos.

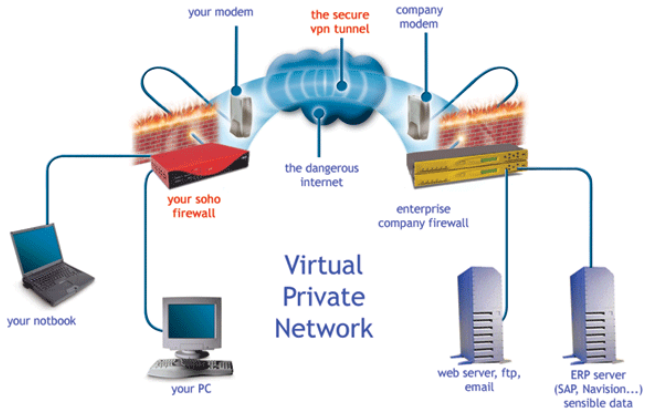
Al correr sobre UDP/IP, L2TP utiliza el puerto 1701. El paquete entero de L2TP, incluyendo la parte de datos y el encabezado, viaja en un datagrama UDP. El que inicia un túnel L2TP toma un puerto UDP de origen que esté disponible, pudiendo ser o no el 1701 y envía a la dirección de destino sobre el puerto 1701. Este extremo toma un puerto libre, que puede ser o no el 1701, y envía la respuesta a la dirección de origen, sobre el mismo puerto iniciador. Luego de

establecida la conexión, los puertos quedan estáticos por el resto de la vida del túnel.

En la autenticación de L2TP, tanto el LAC como el LNS comparten un secreto único. Cada extremo usa este mismo secreto al actuar tanto como autenticado como autenticador.

Sobre la seguridad del paquete L2TP, se requiere que el protocolo de transporte de L2TP tenga la posibilidad de brindar servicios de encriptación, autenticación e integridad para el paquete L2TP en su totalidad. Como tal, L2TP sólo se preocupa por la confidencialidad, autenticidad e integridad de los paquetes L2TP entre los puntos extremos del túnel, no entre los extremos físicos de la conexión.

## SEGURIDAD EN VPN




Para que el uso de VPNs sea seguro se necesita garantizar de alguna manera la autentificación, integridad y confidencialidad durante todo el establecimiento de la comunicación.

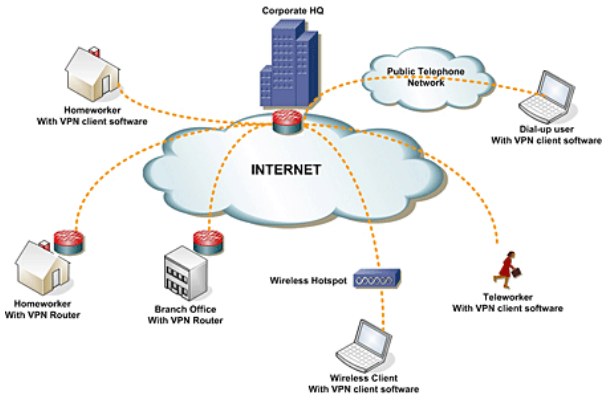
- *Autentificación*: Identificar si el Usuario/equipo está autorizado y hasta qué nivel de acceso le está permitido.

- *Integridad:* Garantizar que los paquetes de datos enviados no fueron modificados o alterados. Para esto se usan herramientas Hash. Los algoritmos hash más conocidos son los Message Digest (MD5) y Secure Hash Algorithm (SHA), entre otros.

- *Confidencialidad*: Asegurar que la información que viaja a través de la VPN sólo puede ser interpretada los receptores. Se utilizan algoritmos de cifrado tales como el Data Encryption Standard (DES), Advanced Encryption Standard (AES), etcétera.

- *No repudio*: Certificar que el usuario que firma el mensaje no puede negar que él es el emisor de ese mensaje.

## SERVICIOS QUE PROVEEN LAS REDES VPN




Al momento de implementar una red, para considerarla una VPN debemos asegurarnos de que ésta proporciona:

- Métodos de Identificación de los usuarios: capacidad de confirmar los datos de sus usuarios y restringir el acceso a los que no estén debidamente autorizados. De igual forma, debe proveer registros que muestren quien accedió, a que información y cuándo.
- Posibildad de administración de direcciones: La red debe proveer de direcciones a sus clientes en la red privada y debe asegurarse de que sean conservadas de esa manera.
- Codificación de los datos en la red: encriptación de los datos que serán enviados a través de la red pública de tal manera que éstos no puedan ser vistos por usuarios sin autorización en la red.
- Administración de claves públicas y privadas: la red privada es la encargada de generar, proveer y renovar las claves de los usuarios de los servidores.
- Soporte a múltiples protocolos existentes: capacidad de la red privada de soportar protocolos comunes utilizados en la red pública. Incluídos el protocolo de internet, el intercambio de paquete de internet, entre otros.

## VENTAJAS Y DESVENTAJAS

Una de las primeras ventajas que existe al momento de utilizar una VPN es que permite a los usuarios hacer uso de una red con las características de la red privada, pero con costos de una red pública. El cliente adquiere en su totalidad, los privilegios de miembro de la red, con lo que se le establecen las reglas y los permisos de un ordenador para esa red privada, pudiendo el usuario tener acceso a la información publicada en la red, como documentos internos, servidores de correo, bases de datos, y más, todo a través de medios

de acceso público, mientras todas las conexiones de acceso a Internet desde el ordenador del cliente de la VPN se realizarán utilizando conexiones y recursos propios de la red privada.

De entre las ventajas más significativas podemos hacer mención de:

- Integridad, confidencialidad, seguridad en los datos transmitidos.

- Reducción de costos y sencillez en el uso de las redes.

- Proporciona facilidades para la comunicación segura de usuarios en lugares distantes.

- Controles de acceso y autenticación basado en políticas de la empresa u organización.

- Opciones de diagnóstico remoto, servicio técnico a distancia.

- Algoritmos de compresión que optimizan el tráfico de los usuarios.

- Permite evitar costos altos de actualizaciones y mantenimiento de PC’s remotas.

Entre las desventajas podemos nombrar:

- Cargas mayores en los clientes debido a que realiza tareas adicionales de encapsulamiento de paquetes una vez más.

- Encriptación de datos produce retardos, lentitud en la red, y sobrecargas del canal de las conexiones de la VPN.

- Aumento de la complejidad de tráfico de paquetes, que pueden generar efectos inesperados o indeseados y que pueden necesitar la realización de modificaciones de las configuraciones de ciertas aplicaciones o algún tipo de programas.

## VPN EN ENTORNOS MOVILES

VPN móvil maneja las circunstancias especiales cuando un extremo de la VPN no es fijo en una sola dirección IP, sino que deambula por diversas redes, tales como redes de datos de las compañías de celulares o entre múltiples puntos de acceso Wi-Fi. VPN móviles han sido ampliamente utilizadas en la seguridad pública, donde dan a los usuarios, acceso a las aplicaciones de misión crítica, tales como el envío de ayuda y datos de criminales, mientras viajan entre diferentes subredes de una red móvil. También se utilizan en la gestión de servicios de campo y en las organizaciones sanitarias, entre otras industrias.

Cada vez más, las VPN móviles están siendo adoptadas por profesionales móviles y los trabajadores de cuello blanco que necesitan conexiones confiables. Permiten a los usuarios moverse sin problemas a través de redes dentro y fuera de las zonas de cobertura inalámbrica sin perder sesiones de la aplicación o dejar caer la sesión VPN segura. Una VPN convencional no pueden sobrevivir estos eventos porque al romperse el túnel, causa la desconexión de las aplicaciones, o incluso hacer que el dispositivo mismo colapse.

En lugar de atar lógicamente el punto final del túnel de red a una dirección IP física, cada túnel está ligado a una dirección IP asociada de forma permanente en el dispositivo. El software de VPN móvil se encarga de la autenticación de red necesarias y mantiene las sesiones de red de forma transparente para la aplicación y el usuario. El anfitrión de identidad Protocolo (HIP), en estudio por la Internet Engineering Task Force, está diseñado para apoyar la movilidad de los ejércitos, separando el papel de las direcciones IP para la identificación de acogida de sus funciones de localización en una red IP. Con HIP un host móvil mantiene sus conexiones lógicas establecidas a través del identificador de la identidad de acogida la que se asocia con diferentes direcciones IP en itinerancia entre redes de acceso.

## Conclusión

Tal como hemos observado, el uso de redes VPN en la actualidad se está expandiendo cada vez más, obteniendo asi el mayor provecho posible de una herramienta que, como comentaba anteriormente, revolucionó el ambiente comercial y empresarial, y la participación de estos en el crecimiento acelerado de las redes y sus tecnologías asociadas.

Las aplicaciones desarrolladas, y en las que se está trabajando en la actualidad demuestran que no sólo el sector comercial-empresarial será el beneficiado con estos avances, sino que como todo desarrollo tecnológico, este también contribuirá con la mejora de nuestra calidad de vida.

## Bibliografía


- **Tanembaum, Andrew.** *Redes de Computadoras.* 4ta Edición. Pearson Prentice Hall, 2003.
- **Stallings, William.** *Data and Computers Networks.* 8va Edición. Pearson Prentice Hall, 2007.
- **Fowler, Dennis.** *Virtual Private Networks: Making the right connection.* 1era Edicion. Morgan Kaufmann Publishers, Inc. 2002.
- **Sitios Web:**
    - http://en.wikipedia.org/wiki/Virtual_private_network
    - http://features.techworld.com/networking/
    - http://compnetworking.about.com/od/vpn/
    - http://www.vpnc.org/vpn-technologies.html
    - http://es.wikipedia.org/vpn

## Anexos

## VPN bajo Demanda

## Conexiones bajo Demanda

Las conexiones bajo demanda se inician sólo posteriormente a que los paquetes IP destinados a una conexión VPN específica intentan fluir. Es decir, la conexión sólo se habilita cuando es necesario. Para estas conexiones se necesita que los filtros de las políticas estén cargados y funcionando, que el servidor de VPN estéen ejecución y que su interfaz esté activa dentro del sistema. Luego de un período de inactividad de la conexión, ésta quedará inactiva esperando el envío de más paquetes IP.

## VPN HAMACHI.

Es una aplicación para crear una VPN (Red Privada Virtual) mediante una conexión de IPs segura con capacidad de transferencia punto a punto. Esto es emular tener dos o más ordenadores conectados a través de internet pero cómo si estuvieses conectado con un cable, estableciendo una conexión segura. No solo sirve para crear Redes Virtuales sólo para juegos, podemos implementarlo estando en nuestro trabajo y así compartir carpetas o archivos con nuestra PC de Hogar. Es un Software muy completo, es totalmente gratuito, traducido a mas de 30 idiomas Compatible con los Sistemas Operativos de Windows® y Linux.

Hamachi consiste en un cluster servidor administrado por el vendedor del sistema y el software cliente, el cual es instalado en los ordenadores de los usuarios.

El software cliente agrega una interfaz de red virtual al ordenador que es utilizada tanto para interceptar el tráfico VPN saliente como para inyectar el tráfico VPN entrante. El tráfico saliente enviado por el sistema operativo a esta interfaz es entregado al software cliente, que lo cifra y lo autentifica y luego lo envía al nodo VPN de destino a través de una conexión UDP iniciada a tal efecto. Hamachi se encarga del tunelamiento del tráfico IP, incluido el broadcast (difusión) y el multicast (multidifusión).

A cada cliente Hamachi se le asigna una dirección IP de la red 5.0.0.0/8. Esta dirección es asignada cuando el cliente se auntentifica en el sistema la primera vez, y es en adelante asociada con la clave de cifrado pública del cliente. Mientras el cliente retenga esta clave, puede autentificarse en el sistema y utilizar esa dirección IP 5.X.X.X.

Hamachi es habitualmente utilizada para jugar en red y para la administración remota. El vendedor provee servicios básicos gratis y otras características extra pagando.

Para que el producto funcione es necesaria la "mediación del servidor", el cual es operado por el vendedor. El servidor almacena el nombre de usuario, contraseña de mantenimiento, dirección IP estática 5.0.0.0/8 y el "token" de autenticación asociado del usuario. Para cada túnel que se establece, podría registrar la dirección IP real del usuario, tiempo de establecimiento y duración; y lo mismo para los demás usuarios interconectados.

***Hamachi*** es una aplicación gratuita configuradora de redes privadas virtuales capaz de establecer vínculos directos entre computadoras que están bajo firewalls de NAT sin requerir reconfiguración. En otras palabras, establece una conexión a través de Internet y simula una red de área local formada por ordenadores remotos. Actualmente está disponible la versión para Microsoft Windows para Mac OS X y Linux.

Hamachi es un sistema de administración redondeada que consiste en un cluster servidor administrado por el vendedor del sistema y el software cliente, el cual es instalado en los ordenadores de los usuarios.

El software cliente agrega una interfaz de red virtual al ordenador que es utilizada tanto para interceptar el tráfico VPN saliente como para inyectar el tráfico VPN entrante. Hamachi se encarga del

tunelamiento del tráfico IP, incluido el broadcast (difusión) y el multicast (multidifusión).

Cada cliente establece y mantiene una conexión de control con el Cluster servidor. Cuando la conexión está establecida, el cliente entra en una secuencia de identificación de usuario, seguida de un proceso de descubrimiento y sincronización de estado. El paso de autentificación de usuario autentifica al cliente contra el servidor y viceversa. El descubrimiento es utilizado para determinar la topología de la conexión a Internet del cliente.

El paso de sincronización extrae una vista del cliente de sus redes privadas sincronizadas con los otros miembros de esas redes. Cuando un miembro de una red se conecta o se desconecta, el servidor da instrucciones a los otros nodos de la red para que inicien o detengan túneles con dicho miembro. Cuando se establecen túneles entre los nodos, Hamachi utiliza una técnica de NAT transversal asistido por servidor.

En el caso de que se pierda la conexión con el servidor de manera inesperada, el cliente mantiene todos sus túneles e inicia una comprobación de sus estados.

Cuando el servidor pierde una conexión de cliente de manera inesperada, se informa a los nodos clientes sobre el hecho y se espera a que inicien sus comprobaciones.

A cada cliente Hamachi se le asigna una dirección OP de la red 5.0.0.0 Esta dirección es asignada cuando el cliente se autentifica en el sistema la primera vez, y es en adelante asociada con la clave de cifrado pública del cliente. Mientras el cliente retenga esta clave, puede autentificarse en el sistema y utilizar esa dirección IP 5.X.X.X

**OpenVPN**

OpenVPN es una solución de conectividad basada en software: SSL (Secure Sockets Layer) VPN Virtual Private Network (red virtual privada), OpenVPN ofrece conectividad punto-a-punto con validación jerárquica de usuarios y host conectados remotamente, resulta una muy buena opción en tecnologías Wi-Fi (redes inalámbricas EEI 802.11) y soporta una amplia configuración, entre ellas balanceo de cargas. Está publicado bajo la licencia GPL, de software libre.

OpenVPN provee seguridad, estabilidad y comprobados mecanismos de cifrado sin sufrir la complejidad de otras soluciones VPN como las de IPsec.

No tiene compatibilidad con IPsec que justamente es el estándar actual para soluciones VPN.
Todavía existe poca gente que conoce como usar OpenVPN.

**TheGreenBow Cliente VPN 4.7**

El Cliente VPN TheGreenBow es un cliente IPSec VPN, compatible con la mayoría de routers VPN populares, y con herramientas de despliegue de seguridad en grandes y medianas empresas. Altamente eficiente y fácil de configurar, el Cliente VPN también permite configuraciones peer-to-peer VPN.
Soporta todos los tipos de conexiones como dial-up, DSL, cable, GSM/GPRS y WiFi.
Posee una Autentificación Fuerte del Usuario, Cifrado fuerte, IP Encapsulating Security y varias características más que permiten una implementación robusta del software.

**Garena**

Es un programa similar al hamachi (VPN por internet) que permite a los usuarios que estén en el mismo canal jugar por red Lan a través de internet.
¿Como se usa?
Simplemente te registras en la pagina (no requiere confirmación), bajas el programa que es muy liviano, lo instalas y logueas. Luego entras en algún canal del juego que queres jugar y listo, a disfrutar.
¿Como funciona?
Garena tiene 5 servidores generales, dentro de cada uno tiene un listado de juegos (después hago la lista abajo) y dentro del juego seleccionado tenes desde 5 a 20 canales (dependiendo del juego), desde sudamericanos, hasta norteamericanos, europeos, asiáticos y demás (beneficiando conectarte con tus vecinos para mejor ping). Te pones de acuerdo con tus amigos, entran al mismo canal y a jugar, o simplemente a jugar con otras personas.
Es uno de los más utilizados y tiene miles de usuarios registrados a nivel mundial. Disponible en varios idiomas es reconocida por ser un lugar en donde se disputan torneos internacionales de los juegos más conocidos como lo son Starcraft, Warcraft, Counter Strike, entre otros. Sin duda es el cliente más desarrollado y el que más funcionalidades presenta para los jugadores.

**Tunngle**

Es un nuevo Virtual VPN desarrollado en Alemania. Esta aplicación presenta una direferencia con Hamachi. Aquí no creas redes a tu conveniencia, sino que ya están creadas por juegos. Esto es, toda la gente que juega a Startcraft se encuentra en un mismo canal.

Se pierde la privacidad de crear canales privados, pero por otro lado, queda toda la gente ahí siempre jugando, siempre hay alguien dispuesto.

Dispone de un sistema de amigos, para ver si los amigos se encuentran online, etc.

Tarda un poco en conectar, pero luego funciona muy bien.

Así como Hamachi usaba el rango de ip's 5.x.x.x , Tunngle usa el 7.x.x.x.